

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/001211

International filing date: 28 January 2005 (28.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-023335
Filing date: 30 January 2004 (30.01.2004)

Date of receipt at the International Bureau: 14 April 2005 (14.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

22.02.2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 1 月 3 0 日
Date of Application:

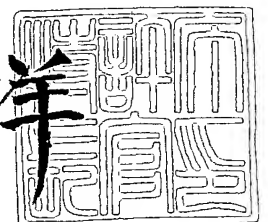
出 願 番 号 特 願 2 0 0 4 - 0 2 3 3 3 5
Application Number:
[ST. 10/C]: [J P 2 0 0 4 - 0 2 3 3 3 5]

出 願 人 日 本 ビ ク タ ー 株 式 会 社
Applicant(s):

2 0 0 5 年 3 月 3 1 日

特 許 庁 長 官
Commissioner,
Japan Patent Office

小 川 洋



【書類名】 特許願
【整理番号】 415001145
【提出日】 平成16年 1月30日
【あて先】 特許庁長官殿
【国際特許分類】 G09C 1/00
H03K 3/84
H04L 9/24

【発明者】
【住所又は居所】 神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地 日本ビクター株
式会社内
【氏名】 猪羽 渉

【発明者】
【住所又は居所】 神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地 日本ビクター株
式会社内
【氏名】 日暮 誠司

【特許出願人】
【識別番号】 000004329
【氏名又は名称】 日本ビクター株式会社

【代理人】
【識別番号】 100083806
【弁理士】
【氏名又は名称】 三好 秀和
【電話番号】 03-3504-3075

【選任した代理人】
【識別番号】 100068342
【弁理士】
【氏名又は名称】 三好 保男

【選任した代理人】
【識別番号】 100101247
【弁理士】
【氏名又は名称】 高橋 俊一

【手数料の表示】
【予納台帳番号】 001982
【納付金額】 21,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9802012

【書類名】特許請求の範囲

【請求項 1】

所定のビット長の擬似乱数列を生成する擬似乱数生成装置であって、
m 段のシフトレジスタを有し、所定のビット長のビット列を出力する第 1 の線形フィードバックシフトレジスタと、

n 段のシフトレジスタを有し、所定のビット長のビット列を出力する第 2 の線形フィードバックシフトレジスタと、

所定の条件に従って、前記第 1 の線形フィードバックシフトレジスタおよび前記第 2 の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値を生成し、それぞれの当該初期値を前記第 1 の線形フィードバックシフトレジスタおよび前記第 2 の線形フィードバックシフトレジスタへ供給する初期値生成手段と、

所定の条件に従って、前記第 2 の線形フィードバックシフトレジスタの特性多項式の係数を生成し、前記第 2 の線形フィードバックシフトレジスタへ供給する多項式係数生成手段と、

前記第 1 の線形フィードバックシフトレジスタの特性多項式として原始多項式を前記原始多項式より少ない情報量の識別番号と共に複数記憶する原始多項式記憶手段と、

所定の条件に従って、前記原始多項式記憶手段に記憶されている原始多項式を 1 つ選択し、その原始多項式の係数を特性多項式の係数として前記第 1 の線形フィードバックシフトレジスタへ供給する原始多項式選択手段と、

前記第 1 の線形フィードバックシフトレジスタから出力されるビット列と、および前記第 2 の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力手段と、
を備えることを特徴とする擬似乱数生成装置。

【請求項 2】

前記擬似乱数生成装置は、

前記原始多項式選択手段によって選択された前記原始多項式の識別番号、前記初期値生成手段によって生成された前記第 1 の線形フィードバックシフトレジスタおよび前記第 2 の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値、前記多項式係数生成手段によって生成された前記特性多項式の係数のそれぞれからなるインisialデータを生成、当該インisialデータを他の擬似乱数生成装置へ送出し、当該インisialデータを他の擬似乱数生成装置から受信した場合は、当該インisialデータから前記第 1 のフィードバックシフトレジスタと前記第 2 のフィードバックシフトレジスタとの各初期値を抽出して前記第 1 の線形フィードバックシフトレジスタと前記第 2 の線形フィードバックシフトレジスタに供給し、当該インisialデータから前記特性多項式の係数を抽出して前記第 2 の線形フィードバックシフトレジスタへ供給し、当該インisialデータから前記原始多項式の識別番号を抽出して前記原始多項式選択手段に供給する通信手段を備え、

前記原始多項式選択手段は、前記通信手段によって抽出された前記識別番号を基に、前記原始多項式記憶手段に記憶されている原始多項式を 1 つ選択し、その原始多項式の係数を前記第 1 の線形フィードバックシフトレジスタへ供給する手段であることを特徴とする請求項 1 に記載の擬似乱数生成装置。

【請求項 3】

所定のビット長の擬似乱数列を生成するコンピュータによって実行される擬似乱数生成プログラムであって、

当該擬似乱数生成プログラムは、前記コンピュータを

m 段のシフトレジスタを有し、所定のビット長のビット列を出力する第 1 の線形フィードバックシフトレジスタと、

n 段のシフトレジスタを有し、所定のビット長のビット列を出力する第 2 の線形フィードバックシフトレジスタと、

所定の条件に従って、前記第 1 の線形フィードバックシフトレジスタおよび前記第 2 の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値を生成し、それ

ぞれの当該初期値を前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタへ供給する初期値生成手段と、

所定の条件に従って、前記第2の線形フィードバックシフトレジスタの特性多項式の係数を生成し、前記第2の線形フィードバックシフトレジスタへ供給する多項式係数生成手段と、

前記第1の線形フィードバックシフトレジスタの特性多項式として原始多項式を前記原始多項式より少ない情報量の識別番号と共に複数記憶する原始多項式記憶手段と、

所定の条件に従って、前記原始多項式記憶手段に記憶されている原始多項式を1つ選択し、その原始多項式の係数を特性多項式の係数として前記第1の線形フィードバックシフトレジスタへ供給する原始多項式選択手段と、

前記第1の線形フィードバックシフトレジスタから出力されるビット列と、および前記第2の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力手段と、

して機能させることを特徴とする擬似乱数生成プログラム。

【請求項4】

前記擬似乱数生成プログラムは、前記コンピュータを

前記原始多項式選択手段によって選択された前記原始多項式の識別番号、前記初期値生成手段によって生成された前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値、前記多項式係数生成手段によって生成された前記特性多項式の係数のそれぞれからなるイニシャルデータを生成、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第1のフィードバックシフトレジスタと前記第2のフィードバックシフトレジスタとの各初期値を抽出して前記第1の線形フィードバックシフトレジスタと前記第2の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記特性多項式の係数を抽出して前記第2の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別番号を抽出して前記原始多項式選択手段に供給する通信手段としても機能させ、

前記原始多項式選択手段は、前記通信手段によって抽出された前記識別番号を基に、前記原始多項式記憶手段に記憶されている原始多項式を1つ選択し、その原始多項式の係数を前記第1の線形フィードバックシフトレジスタへ供給する手段であることを特徴とする請求項3に記載の擬似乱数生成プログラム。

【書類名】明細書

【発明の名称】擬似乱数生成装置および擬似乱数生成プログラム

【技術分野】

【0001】

本発明は、暗号通信に利用される擬似乱数を生成する擬似乱数生成装置および擬似乱数生成プログラムに関する。

【背景技術】

【0002】

現在、電話や無線、インターネット等におけるデータ通信では、通信されるデータを第三者による盗聴や改ざんから保護するために、データの暗号化が行われている。データの送信側では、暗号鍵を用いて送信するデータを暗号化した後送信し、受信側では、その暗号化されたデータを受信すると、復号鍵を用いて復号化しデータを得ている。もしこの時、第三者がデータを傍受しても、正当な復号鍵を持たないため暗号化されたデータを復号することができず、また、意図したデータの改ざんを行うこともできない。

【0003】

このような暗号化の方式には、共通鍵暗号方式や公開鍵暗号方式があり、それぞれの特徴をいかして利用される条件に応じて選択される。いずれの方式であっても、暗号鍵によって通信されるデータの安全性が保障されており、その暗号鍵は容易に推測されないように擬似乱数を用いる方法が知られている。

【0004】

例えば、線形フィードバックシフトレジスタによる擬似乱数の生成方法では、乱数生成のための比較的短い初期値からデータ長の長い擬似乱数列を生成することができるため、複数の装置で同じ擬似乱数を生成しようとするとき、初期値を共有するだけで良い。また、一般に、特定の条件を満たす原始多項式を特性多項式とする複数の線形フィードバックシフトレジスタを組み合わせることで、生成される擬似乱数の予測が困難な擬似乱数生成装置を実現可能なが知られている。さらに、初期値を共有しなくても、複数の線形フィードバックシフトレジスタの選択情報を共有化することで、同じ擬似乱数列を生成することも可能である（特許文献1）。

【0005】

しかしながら、線形フィードバックシフトレジスタを用いた擬似乱数生成装置では、たとえ非線形な処理を組み合わせた方法であっても、ある特定のアルゴリズムで擬似乱数が生成されるため、初期値や生成される擬似乱数列の一部からその後生成される擬似乱数が推測される恐れがあった。

【0006】

また、複数の線形フィードバックシフトレジスタからいくつかのレジスタを選択して擬似乱数を生成する場合には、生成される擬似乱数列の推測は困難になるものの、任意の係数を特性多項式とする線形フィードバックシフトレジスタを組み合わせると、生成される擬似乱数列が必ずしもM系列（Maximal-length sequences）とはならず、短い周期で同じ擬似乱数列を繰り返し生成してしまうという問題があるため、予め特定の条件を満たす多項式を多数用意した中から選択して組み合わせる必要があった。これは実際の処理では、常に利用するわけではない線形フィードバックシフトレジスタを実装する必要があり効率的ではなかった。

【特許文献1】特開平10-91066号公報

【特許文献2】特開平10-93548号公報

【特許文献3】特開2000-81969号公報

【発明の開示】

【発明が解決しようとする課題】

【0007】

本発明は、生成される擬似乱数列や送受信されるデータを観測されても、その後生成される擬似乱数列の推測が困難な暗号通信に好適な擬似乱数生成装置および擬似乱数生成プ

プログラムを提供することを目的とする。

【課題を解決するための手段】

【0008】

上記目的を達成するために、請求項1に記載の擬似乱数生成装置は、所定のビット長の擬似乱数列を生成する擬似乱数生成装置であって、m段のシフトレジスタを有し、所定のビット長のビット列を出力する第1の線形フィードバックシフトレジスタと、n段のシフトレジスタを有し、所定のビット長のビット列を出力する第2の線形フィードバックシフトレジスタと、所定の条件に従って、前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値を生成し、それぞれの当該初期値を前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタへ供給する初期値生成手段と、所定の条件に従って、前記第2の線形フィードバックシフトレジスタの特性多項式の係数を生成し、前記第2の線形フィードバックシフトレジスタへ供給する多項式係数生成手段と、前記第1の線形フィードバックシフトレジスタの特性多項式として原始多項式を前記原始多項式より少ない情報量の識別番号と共に複数記憶する原始多項式記憶手段と、所定の条件に従って、前記原始多項式記憶手段に記憶されている原始多項式を1つ選択し、その原始多項式の係数を特性多項式の係数として前記第1の線形フィードバックシフトレジスタへ供給する原始多項式選択手段と、前記第1の線形フィードバックシフトレジスタから出力されるビット列と、および前記第2の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力手段とを備えることを特徴とする。

【0009】

また、請求項2に記載の擬似乱数生成装置は、請求項1に記載の擬似乱数生成装置であって、前記擬似乱数生成装置は、前記原始多項式選択手段によって選択された前記原始多項式の識別番号、前記初期値生成手段によって生成された前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値、前記多項式係数生成手段によって生成された前記特性多項式の係数のそれぞれからなるイニシャルデータを生成、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第1のフィードバックシフトレジスタと前記第2のフィードバックシフトレジスタとの各初期値を抽出して前記第1の線形フィードバックシフトレジスタと前記第2の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記特性多項式の係数を抽出して前記第2の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別番号を抽出して前記原始多項式選択手段に供給する通信手段を備え、前記原始多項式選択手段は、前記通信手段によって抽出された前記識別番号を基に、前記原始多項式記憶手段に記憶されている原始多項式を1つ選択し、その原始多項式の係数を前記第1の線形フィードバックシフトレジスタへ供給する手段であることを特徴とする。

【0010】

また、請求項3に記載の擬似乱数生成プログラムは、所定のビット長の擬似乱数列を生成するコンピュータによって実行される擬似乱数生成プログラムであって、当該擬似乱数生成プログラムは、前記コンピュータをm段のシフトレジスタを有し、所定のビット長のビット列を出力する第1の線形フィードバックシフトレジスタと、n段のシフトレジスタを有し、所定のビット長のビット列を出力する第2の線形フィードバックシフトレジスタと、所定の条件に従って、前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値を生成し、それぞれの当該初期値を前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタへ供給する初期値生成手段と、所定の条件に従って、前記第2の線形フィードバックシフトレジスタの特性多項式の係数を生成し、前記第2の線形フィードバックシフトレジスタへ供給する多項式係数生成手段と、前記第1の線形フィ

ードバックシフトレジスタの特性多項式として原始多項式を前記原始多項式より少ない情報量の識別番号と共に複数記憶する原始多項式記憶手段と、所定の条件に従って、前記原始多項式記憶手段に記憶されている原始多項式を1つ選択し、その原始多項式の係数を特性多項式の係数として前記第1の線形フィードバックシフトレジスタへ供給する原始多項式選択手段と、前記第1の線形フィードバックシフトレジスタから出力されるビット列と、および前記第2の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力手段として機能させることを特徴とする。

【0011】

また、請求項4に記載の擬似乱数生成プログラムは、請求項3に記載の擬似乱数生成プログラムであって、前記擬似乱数生成プログラムは、前記コンピュータを前記原始多項式選択手段によって選択された前記原始多項式の識別番号、前記初期値生成手段によって生成された前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値、前記多項式係数生成手段によって生成された前記特性多項式の係数のそれぞれからなるイニシャルデータを生成、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第1のフィードバックシフトレジスタと前記第2のフィードバックシフトレジスタとの各初期値を抽出して前記第1の線形フィードバックシフトレジスタと前記第2の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記特性多項式の係数を抽出して前記第2の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別番号を抽出して前記原始多項式選択手段に供給する通信手段としても機能させ、前記原始多項式選択手段は、前記通信手段によって抽出された前記識別番号を基に、前記原始多項式記憶手段に記憶されている原始多項式を1つ選択し、その原始多項式の係数を前記第1の線形フィードバックシフトレジスタへ供給する手段であることを特徴とする。

【発明の効果】

【0012】

本発明によれば、常に所定のM系列より長い周期の擬似乱数列を生成することが可能となり、初期値だけでなく、特性多項式の係数も任意に設定できるため、生成された擬似乱数列を観測されてもその後生成される擬似乱数列を推測することは困難であり、生成される擬似乱数列の安全性を確保することができ、通信されるデータの安全性が保障される。

【0013】

また、第1の線形フィードバックシフトレジスタの特性多項式として設定される原始多項式の選択には、その識別情報を用いることにより、係数を送受信するより少ないデータ量で済む。

【発明を実施するための最良の形態】

【0014】

本発明の実施形態を、図1～図9を用いて説明する。なお、擬似乱数生成装置1が生成する擬似乱数のビット長を $h+1$ とする。

【0015】

＜第1の実施形態＞

第1の実施形態における擬似乱数生成装置1は、図1に示すように、第1線形フィードバックシフトレジスタ2、第2線形フィードバックシフトレジスタ3、初期値生成部4、多項式係数生成部5、および擬似乱数出力部6を有する。

【0016】

第1線形フィードバックシフトレジスタ2は、 m 次の線形フィードバックシフトレジスタであり、 m 個のフリップフロップ回路を有する（詳細については後述）。また、第2線形フィードバックシフトレジスタ3は、 n 次の線形フィードバックシフトレジスタであり、 n 個のフリップフロップ回路を有する（詳細については後述）。

【0017】

初期値生成部 4 は、外部から入力される初期情報、あるいは予め定められた所定の条件、例えば、日時情報のように常に変化する情報や熱雑音等の物理現象を利用して得られる条件に従って、第 1 線形フィードバックシフトレジスタ 2 を構成する各フリップフロップの初期値 ia ($ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0$) を生成し、第 1 線形フィードバックシフトレジスタ 2 へ供給する機能、第 2 線形フィードバックシフトレジスタ 3 を構成する各フリップフロップの初期値 ib ($ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0$) を生成し、第 2 線形フィードバックシフトレジスタ 3 へ供給する機能を有する。ただし、第 2 線形フィードバックシフトレジスタ 3 からの出力が常に“0”にならないよう、少なくとも初期値 $ia_{m-1} \sim ia_0$ のいずれか 1 つが値“1”であり、同様に、少なくとも初期値 $ib_{n-1} \sim ib_0$ のいずれか 1 つが値“1”であることとする。

【0018】

また、多項式係数生成部 5 は、外部から入力される初期情報、あるいは予め定められた所定の条件、例えば、日時情報のように常に変化する情報や熱雑音等の物理現象を利用して得られる条件に従って、第 2 線形フィードバックシフトレジスタ 3 の特性多項式の係数 s ($s_{n-1}, s_{n-2}, \dots, s_2, s_1$) を生成し、第 2 線形フィードバックシフトレジスタ 3 へ供給する機能を有する。

【0019】

また、擬似乱数出力部 6 は、第 1 線形フィードバックシフトレジスタ 2 から順次出力されるビット列 ra ($ra_0, ra_1, \dots, ra_{h-1}, ra_h$) と、および第 2 線形フィードバックシフトレジスタ 3 から順次出力されるビット列 rb ($rb_0, rb_1, \dots, rb_{h-1}, rb_h$) とに基づいて、各ビットの排他的論理和を求め所定のビット長の擬似乱数 r ($r_0, r_1, \dots, r_{h-1}, r_h$) を生成し、出力する機能を有する。

【0020】

第 1 線形フィードバックシフトレジスタ 2 は、図 2 に示すように、 m 個のフリップフロップ回路と AND 回路、および XOR 回路から構成される。この第 1 線形フィードバックシフトレジスタ 2 の特性多項式は、予め定められた原始多項式 $a_m x^m + a_{m-1} x^{m-1} + a_{m-2} x^{m-2} + \dots + a_2 x^2 + a_1 x + a_0$ (ただし、 $a_m=1$) であり、AND 回路それぞれに原始多項式の係数 a (a_{m-1}, \dots, a_1) が設定される。

【0021】

従って、 $a_i=0$ ($0 < i < m$) の時は、フリップフロップ FA_{i-1} ($0 < i < m$) から出力される値に関係なく AND 回路からは“0”が出力され、 $a_i=1$ ($0 < i < m$) の時は、フリップフロップ FA_{i-1} ($0 < i < m$) から出力される値が出力される。

【0022】

第 2 線形フィードバックシフトレジスタ 3 は、図 3 に示すように、 n 個のフリップフロップ回路と AND 回路、および XOR 回路から構成される。この第 2 線形フィードバックシフトレジスタ 3 の特性多項式を $b_n x^n + b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \dots + b_2 x^2 + b_1 x + b_0$ とすると、AND 回路それぞれに特性多項式の係数 b (b_{n-1}, \dots, b_1 =係数 s) が設定される。

【0023】

従って、 $b_j=0$ ($0 < j < n$) の時は、フリップフロップ FB_{j-1} ($0 < j < n$) から出力される値に関係なく AND 回路からは“0”が出力され、 $b_j=1$ ($0 < j < n$) の時は、フリップフロップ FB_{j-1} ($0 < j < n$) から出力される値が出力される。

【0024】

次に、擬似乱数生成装置 1 A の動作について、図 4 のフローチャートに基づいて説明する。

【0025】

擬似乱数生成装置 1 A が擬似乱数生成の処理を開始すると、まず、初期値生成部 4 が、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、初期値 ia ($ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0$) と初期値 ib ($ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0$) を生成し (ステップ S01)、それぞれの初期値を第 1 線形フィードバックシフトレジスタ 2 と第 2 線形フィードバックシフトレジスタ 3 へ供給する。

【0026】

また、多項式係数生成部 5 が、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、第 2 線形フィードバックシフトレジスタ 3 の特性多項式の係数 s ($s_{n-1}, s_{n-2}, \dots, s_2, s_1$) を生成し (ステップ S 0 2)、第 2 線形フィードバックシフトレジスタ 3 へ供給する。

【0027】

第 1 線形フィードバックシフトレジスタ 2 と第 2 線形フィードバックシフトレジスタ 3 は、初期値生成部 4 と多項式係数生成部 5 から各初期値と係数が供給されると、各フリップフロップ回路と AND 回路に各初期値と係数を設定し、出力ビット数をカウントするカウンタ k の値を $k=0$ に設定する (ステップ S 0 3)。第 1 線形フィードバックシフトレジスタ 2 の各フリップフロップ回路 $FA_{n-1}, FA_{n-2}, \dots, FA_1, FA_0$ には、初期値 ia ($ia_{n-1}, ia_{n-2}, \dots, ia_1, ia_0$) が設定され、各 AND 回路には、原始多項式の係数 a (a_{n-1}, \dots, a_1) が設定される。また、第 2 線形フィードバックシフトレジスタ 3 の各フリップフロップ回路 $FB_n, FB_{n-1}, \dots, FB_1, FB_0$ には、初期値 ib ($ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0$) が設定され、各 AND 回路には、特性多項式の係数 s ($s_{n-1}, s_{n-2}, \dots, s_2, s_1$) が設定される。なお、図 3 の第 2 線形フィードバックシフトレジスタ 3 では、 $b_n=1, b_0=1$ としているが、 b_n および b_0 に AND 回路を設けて、他の係数と同様に任意の値を設定できるようにしてもよい。

【0028】

次に、第 1 線形フィードバックシフトレジスタ 2 にクロック信号を入力すると (ステップ S 0 4)、第 1 線形フィードバックシフトレジスタ 2 は演算を行い、ビット ra_k を出力する (ステップ S 0 5)。同様に、第 2 線形フィードバックシフトレジスタ 3 にクロック信号を入力すると (ステップ S 0 6)、第 2 線形フィードバックシフトレジスタ 3 は演算を行い、ビット rb_k を出力する (ステップ S 0 7)。

【0029】

擬似乱数出力部 6 は、第 1 線形フィードバックシフトレジスタ 2 からビット ra_k が出力され、第 2 線形フィードバックシフトレジスタ 3 からビット rb_k が出力されると、両ビット値の排他的論理和を求めビット r_k を生成する (ステップ S 0 8)。

【0030】

次に、第 1 線形フィードバックシフトレジスタ 2 と第 2 線形フィードバックシフトレジスタ 3 は、カウンタ k の値を 1 つインクリメント ($k \leftarrow k+1$) し (ステップ S 0 9)、カウンタ k の値が h の値を超えたかどうか判定する (ステップ S 1 0)。カウンタ k の値が h 以下の場合には、第 1 線形フィードバックシフトレジスタ 2 はステップ S 0 4 に戻ってビット ra_{k+1} を出力し、第 2 線形フィードバックシフトレジスタ 3 はステップ S 0 6 に戻ってビット rb_{k+1} を出力し、擬似乱数出力部 6 は、ビット r_{k+1} を生成する。

【0031】

カウンタ k の値が h より大きい場合は、擬似乱数生成装置 1 は擬似乱数生成処理を終了し、これまでに生成されたビット $r_0, r_1, \dots, r_{h-1}, r_h$ が擬似乱数 r ($r_0, r_1, \dots, r_{h-1}, r_h$) として出力される (ステップ S 1 1)。

【0032】

ここで、図 5 を用いて具体的に説明する。一例として、8 ビットの擬似乱数 r を出力するものとし、第 1 線形フィードバックシフトレジスタ 2 の原始多項式を x^7+x^3+1 とし、第 1 線形フィードバックシフトレジスタ 2 のフリップフロップ回路を 7 段構成として初期値 ia ($ia_6, ia_5, \dots, ia_1, ia_0$) = (1, 0, 1, 0, 1, 0, 1)、第 2 線形フィードバックシフトレジスタ 3 のフリップフロップ回路を 8 段構成として初期値 ib ($ib_7, ib_6, \dots, ib_1, ib_0$) = (1, 1, 1, 1, 0, 0, 0, 0)、第 2 線形フィードバックシフトレジスタ 3 の特性多項式の係数 s ($s_7, s_6, \dots, s_2, s_1$) = (0, 1, 1, 1, 0, 1, 1) がそれぞれ設定されたとする。

【0033】

まず、1 回目のクロック信号が入力されると、第 1 線形フィードバックシフトレジスタ 2 においては、 $FA_0 \rightarrow FA_1, FA_1 \rightarrow FA_2, \dots, FA_5 \rightarrow FA_6$ とビットがシフトして ($FA_6, FA_5, FA_4, FA_3, FA_2, FA_1$) = (0, 1, 0, 1, 0, 1) となる。第 1 線形フィードバックシフトレジスタ 2 の原

始多項式を x^7+x^3+1 なので、 FA_6 のビット“1”は FA_2 から FA_3 へ出力されるビット“1”との排他的論理和“0”を FA_0 にフィードバックして図5の+1の状態になり、第1線形フィードバックシフトレジスタ2は“0”を ra_0 として出力する。

【0034】

また、1回目のクロック信号が入力されると、第2線形フィードバックシフトレジスタ3においては、 $FB_0 \rightarrow FB_1$ 、 $FB_1 \rightarrow FB_2$ 、 \dots 、 $FB_6 \rightarrow FB_7$ とビットがシフトして $(FB_7, FB_6, FB_5, FB_4, FB_3, FB_2, FB_1) = (1, 1, 1, 0, 0, 0, 0)$ となる。特性多項式の係数 s ($s_7, s_6, \dots, s_2, s_1$) = $(0, 1, 1, 1, 0, 1, 1)$ から、特性多項式は $x^8+x^6+x^5+x^4+x^2+x+1$ なので、 FB_5 から FB_6 へ出力されるビット“1”と、 FB_3 から FB_4 へ出力されるビット“0”と、 FB_1 から FB_2 へ出力されるビット“0”と、 FB_0 から FB_1 へ出力されるビット“0”との排他的論理和“1”を FB_0 にフィードバックして図5の+1の状態になり、第2線形フィードバックシフトレジスタ3は“1”を rb_0 として出力する。

【0035】

2回目のクロック信号が入力されると、第1線形フィードバックシフトレジスタ2および第2線形フィードバックシフトレジスタ3は、同様にビットシフトを行い、原始多項式と特性多項式に基づいてフィードバックを行い、図5の+2の状態となり、それぞれ $ra_1=0$ および $rb_1=1$ を出力する。

【0036】

このように演算を繰り返すことによって、第1線形フィードバックシフトレジスタ2からは $(ra_0, ra_1, \dots, ra_6, ra_7) = (0, 0, 0, 0, 1, 0, 1, 1)$ 、第2線形フィードバックシフトレジスタ3からは $(rb_0, rb_1, \dots, rb_6, rb_7) = (1, 1, 1, 1, 1, 0, 0, 1)$ が出力され、 $(ra_0, ra_1, \dots, ra_6, ra_7) = (0, 0, 0, 0, 1, 0, 1, 1)$ と $(rb_0, rb_1, \dots, rb_6, rb_7) = (1, 1, 1, 1, 1, 0, 0, 1)$ との排他的論理和から擬似乱数 r ($r_0, r_1, \dots, r_6, r_7$) = $(1, 1, 1, 1, 0, 0, 1, 0)$ が出力される。

【0037】

《第2の実施形態》

第2の実施形態における擬似乱数生成装置1Bは、図6に示すように、第1線形フィードバックシフトレジスタ2、第2線形フィードバックシフトレジスタ3、初期値生成部4、多項式係数生成部5、擬似乱数出力部6、原始多項式選択部7、および原始多項式記憶部8を有する。なお、第1の実施形態と同じものについては、同じ番号を付し、その詳細な説明を省略する。

【0038】

原始多項式選択部7は、外部から入力される初期情報に従って、原始多項式記憶部8に記憶されている原始多項式を1つ選択し、特性多項式としてその原始多項式の係数 a (a_{m-1}, \dots, a_1)を第1線形フィードバックシフトレジスタ2へ供給する機能を有する。

【0039】

原始多項式記憶部8は、第1線形フィードバックシフトレジスタ2の各AND回路を設定するための原始多項式を識別番号と共に複数記憶する。この識別番号によって、原始多項式の係数より少ない情報量で各AND回路を設定することが可能であり、例えば、図6に示すように、ビット長を2ビットとすると、原始多項式記憶部8は、識別番号No. “00”は x^7+x^3+1 、識別番号No. “01”は $x^7+x^3+x^2+x+1$ 、識別番号No. “10”は $x^7+x^4+x^3+x^2+1$ 、識別番号No. “11”は $x^7+x^6+x^5+x^4+x^2+x+1$ というような原始多項式を記憶する。

【0040】

次に、擬似乱数生成装置1Bの動作について、図7のフローチャートに基づいて説明する。

【0041】

擬似乱数生成装置1Bが擬似乱数生成の処理を開始すると、まず、原始多項式選択部7が、外部から入力される初期情報に従って、原始多項式記憶部8から原始多項式を1つ選択し(ステップS21)、その選択した原始多項式の係数を特性多項式の係数 a (a_{m-1}, \dots, a_1)として第1線形フィードバックシフトレジスタ2へ供給する。

【0042】

また、初期値生成部 4 は、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、初期値 ia ($ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0$) と初期値 ib ($ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0$) を生成し (ステップ S 2 2)、それぞれの初期値を第 1 線形フィードバックシフトレジスタ 2 と第 2 線形フィードバックシフトレジスタ 3 へ供給する。

【0043】

また、多項式係数生成部 5 が、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、第 2 線形フィードバックシフトレジスタ 3 の特性多項式の係数 s ($s_{n-1}, s_{n-2}, \dots, s_2, s_1$) を生成し (ステップ S 2 3)、第 2 線形フィードバックシフトレジスタ 3 へ供給する。

【0044】

第 1 線形フィードバックシフトレジスタ 2 と第 2 線形フィードバックシフトレジスタ 3 は、原始多項式選択部 7、初期値生成部 4、および多項式係数生成部 5 から各初期値と係数が供給されると、各フリップフロップ回路と AND 回路に各初期値と係数を設定し、出力ビット数をカウントするカウンタ k の値を $k=0$ に設定する (ステップ S 2 4)。第 1 線形フィードバックシフトレジスタ 2 の各フリップフロップ回路 $FA_{m-1}, FA_{m-2}, \dots, FA_1, FA_0$ には、初期値 ia ($ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0$) が設定され、各 AND 回路には、原始多項式選択部 7 から供給された特性多項式の係数 a (a_{m-1}, \dots, a_1) が設定される。また、第 2 線形フィードバックシフトレジスタ 3 の各フリップフロップ回路 $FB_{n-1}, FB_{n-2}, \dots, FB_1, FB_0$ には、初期値 ib ($ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0$) が設定され、各 AND 回路には、特性多項式の係数 s ($s_{n-1}, s_{n-2}, \dots, s_2, s_1$) が設定される。なお、図 3 の第 2 線形フィードバックシフトレジスタ 3 では、 $b_n=1, b_0=1$ としているが、 b_n および b_0 に AND 回路を設けて、他の係数と同様に任意の値を設定できるようにしてもよい。

【0045】

以降、第 1 の実施形態 (ステップ S 0 4 ~ ステップ S 1 1) と同様の処理を行って擬似乱数 r ($r_0, r_1, \dots, r_{h-1}, r_h$) を出力する (ステップ S 2 5 ~ ステップ S 3 2)。

【0046】

＜第 3 の実施形態＞

第 3 の実施形態として、2 つの擬似乱数生成装置 1、例えば送信装置側に設けられた擬似乱数生成装置 1 と受信装置側に設けられた擬似乱数生成装置 1 とで特性多項式の係数と初期値 (イニシャルデータ) を共有して、同じ擬似乱数を生成する擬似乱数生成装置 1 C を示す。

【0047】

第 3 の実施形態における擬似乱数生成装置 1 C は、図 8 に示すように、第 1 線形フィードバックシフトレジスタ 2、第 2 線形フィードバックシフトレジスタ 3、初期値生成部 4、多項式係数生成部 5、擬似乱数出力部 6、原始多項式選択部 7、原始多項式記憶部 8、および通信部 9 を有する。なお、第 1 の実施形態および第 2 の実施形態と同じものについては、同じ番号を付し、その詳細な説明を省略する。また、便宜的に、イニシャルデータ送信側の擬似乱数生成装置 1 の構成要件には “t” の文字を、イニシャルデータ受信側の擬似乱数生成装置 1 の構成要件には “r” の文字を付す。

【0048】

通信部 9 は、原始多項式選択部 7 が選択した原始多項式の識別番号、初期値生成部 4 が生成した初期値 ia ($ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0$) および初期値 ib ($ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0$)、多項式係数生成部 5 が生成した特性多項式の係数 s ($s_{n-1}, s_{n-2}, \dots, s_2, s_1$) を基に、原始多項式の識別番号、特性多項式の係数の初期値、および各初期値のそれぞれのビット列からなるイニシャルデータを生成する機能、およびそのイニシャルデータを他の擬似乱数生成装置 1 と送受信する機能を有する。

【0049】

また、通信部 9 は、イニシャルデータを受信した場合は、イニシャルデータから初期値 ib ($ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0$) と特性多項式の係数 s ($s_{n-1}, s_{n-2}, \dots, s_2, s_1$) とを抽出し、第 2 線形フィードバックシフトレジスタ 3 に供給する機能、イニシャルデータから初期

値 $ia (ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0)$ を抽出し、第1線形フィードバックシフトレジスタ2に供給する機能、イニシャルデータから原始多項式の識別番号を抽出し、原始多項式選択部7に供給する機能を有する。

【0050】

次に、2つの擬似乱数生成装置1Cで同じ擬似乱数を生成する際の動作について、図9のシーケンス図に基づいて説明する。

【0051】

擬似乱数生成装置1Ctが擬似乱数生成の処理を開始すると、まず、原始多項式選択部7tが、外部から入力される初期情報に従って、原始多項式記憶部8tから原始多項式を1つ選択し（ステップS41）、その選択した原始多項式の係数を特性多項式の係数 $a (a_{m-1}, \dots, a_1)$ として第1線形フィードバックシフトレジスタ2tへ供給すると共に、通信部9tへ原始多項式の識別番号を供給する。

【0052】

また、初期値生成部4tは、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、初期値 $ia (ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0)$ と初期値 $ib (ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0)$ を生成し（ステップS42）、それぞれの初期値を第1線形フィードバックシフトレジスタ2t、第2線形フィードバックシフトレジスタ3t、および通信部9tへ供給する。

【0053】

また、多項式係数生成部5tが、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、第2線形フィードバックシフトレジスタ3tの特性多項式の係数 $s (s_{n-1}, s_{n-2}, \dots, s_2, s_1)$ を生成し（ステップS43）、第2線形フィードバックシフトレジスタ3tと通信部9tへ供給する。

【0054】

第1線形フィードバックシフトレジスタ2tと第2線形フィードバックシフトレジスタ3tは、原始多項式選択部7t、初期値生成部4t、および多項式係数生成部5tから各初期値と係数が供給されると、各フリップフロップ回路とAND回路に各初期値と係数を設定し、出力ビット数をカウントするカウンタkの値を $k=0$ に設定する（ステップS44）。第1線形フィードバックシフトレジスタ2tの各フリップフロップ回路 $FA_{m-1}, FA_{m-2}, \dots, FA_1, FA_0$ には、初期値 $ia (ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0)$ が設定され、各AND回路には、原始多項式選択部7tから供給された特性多項式の係数 $a (a_{m-1}, \dots, a_1)$ が設定される。また、第2線形フィードバックシフトレジスタ3tの各フリップフロップ回路 $FB_{n-1}, FB_{n-2}, \dots, FB_1, FB_0$ には、初期値 $ib (ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0)$ が設定され、各AND回路には、特性多項式の係数 $s (s_{n-1}, s_{n-2}, \dots, s_2, s_1)$ が設定される。なお、図3の第2線形フィードバックシフトレジスタ3tでは、 $b_n=1, b_0=1$ としているが、 b_n および b_0 にAND回路を設けて、他の係数と同様に任意の値を設定できるようにしてもよい。

【0055】

また、通信部9tは、原始多項式の識別番号、特性多項式の係数、および各初期値のそれぞれのビット値からなるイニシャルデータを生成し擬似乱数生成装置1Crへ送信する（ステップS45）。この時、通信部9tは、所定の暗号化方式でイニシャルデータを暗号化して送信しても良い。

【0056】

例えば、原始多項式の識別番号が2ビット（“10”）、初期値 ia が7ビット（“1010101”）、初期値 ib が8ビット（“11110000”）、特性多項式の係数 s が7ビット（“0111011”）であった場合、イニシャルデータは24ビットのデータ列（識別番号|初期値 ia |初期値 ib |係数 s ）=（101010101111100000111011）となる。

【0057】

以降、擬似乱数生成装置1Ctは、第1の実施形態（ステップS04～ステップS11）と同様の処理を行って擬似乱数 $r (r_0, r_1, \dots, r_{h-1}, r_h)$ を出力する（ステップS46～ステップS51）。

【0058】

一方、擬似乱数生成装置 1 C r の通信部 9 r は、擬似乱数生成装置 1 C t からインシヤルデータを受信すると（ステップ S 5 2）、インシヤルデータから初期値 ib ($ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0$) と特性多項式の係数 s ($s_{n-1}, s_{n-2}, \dots, s_2, s_1$) とを抽出し、第 2 線形フィードバックシフトレジスタ 3 r に供給し、インシヤルデータから初期値 ia ($ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0$) を抽出し、第 1 線形フィードバックシフトレジスタ 2 r に供給し、インシヤルデータから原始多項式の識別番号を抽出し、原始多項式選択部 7 r に供給する。なお、受信したインシヤルデータが暗号化されている場合は、通信部 9 は、復号化してインシヤルデータを得る。

【0059】

原始多項式選択部 7 r は、原始多項式の識別番号が供給されると、その識別番号に該当する原始多項式を原始多項式記憶部 8 r から 1 つ選択し（ステップ S 5 3）、その選択した原始多項式の係数を特性多項式の係数 a (a_{m-1}, \dots, a_1) として第 1 線形フィードバックシフトレジスタ 2 r へ供給する。

【0060】

また、第 1 線形フィードバックシフトレジスタ 2 r と第 2 線形フィードバックシフトレジスタ 3 r は、原始多項式選択部 7 r、および通信部 9 r から各初期値と各係数が供給されると、各フリップフロップ回路と AND 回路に各初期値と係数を設定し、出力ビット数をカウントするカウンタ k の値を $k=0$ に設定する（ステップ S 5 4）。

【0061】

以降、擬似乱数生成装置 1 C r は、第 1 の実施形態（ステップ S 0 4～ステップ S 1 1）と同様の処理を行って擬似乱数 r ($r_0, r_1, \dots, r_{h-1}, r_h$) を出力する（ステップ S 5 5～ステップ S 6 0）。

【0062】

このようにして、2 つの擬似乱数生成装置 1 でインシヤルデータを共有することによって、同じ擬似乱数を生成することが可能となる。

【0063】

なお、擬似乱数生成装置 1 は、上記の機能を記述した擬似乱数生成プログラムを汎用コンピュータに実行させることによって実現させても良い。この擬似乱数生成プログラムは、記録媒体から読み取られて汎用コンピュータに実行されても良いし、ネットワークを介して外部から伝送されて汎用コンピュータに実行されても良い。

【図面の簡単な説明】

【0064】

【図 1】 擬似乱数生成装置 A の機能構成を示す図である。

【図 2】 第 1 線形フィードバックシフトレジスタの回路構成を示す図である。

【図 3】 第 2 線形フィードバックシフトレジスタの回路構成を示す図である。

【図 4】 第 1 の実施形態における擬似乱数生成の処理を示すフローチャートである。

【図 5】 第 1 線形フィードバックシフトレジスタと第 2 線形フィードバックシフトレジスタの値の遷移を示す図である。

【図 6】 擬似乱数生成装置 B の機能構成を示す図である。

【図 7】 第 2 の実施形態における擬似乱数生成の処理を示すフローチャートである。

【図 8】 擬似乱数生成装置 C の機能構成を示す図である。

【図 9】 第 3 の実施形態における擬似乱数生成の処理を示すシーケンス図である。

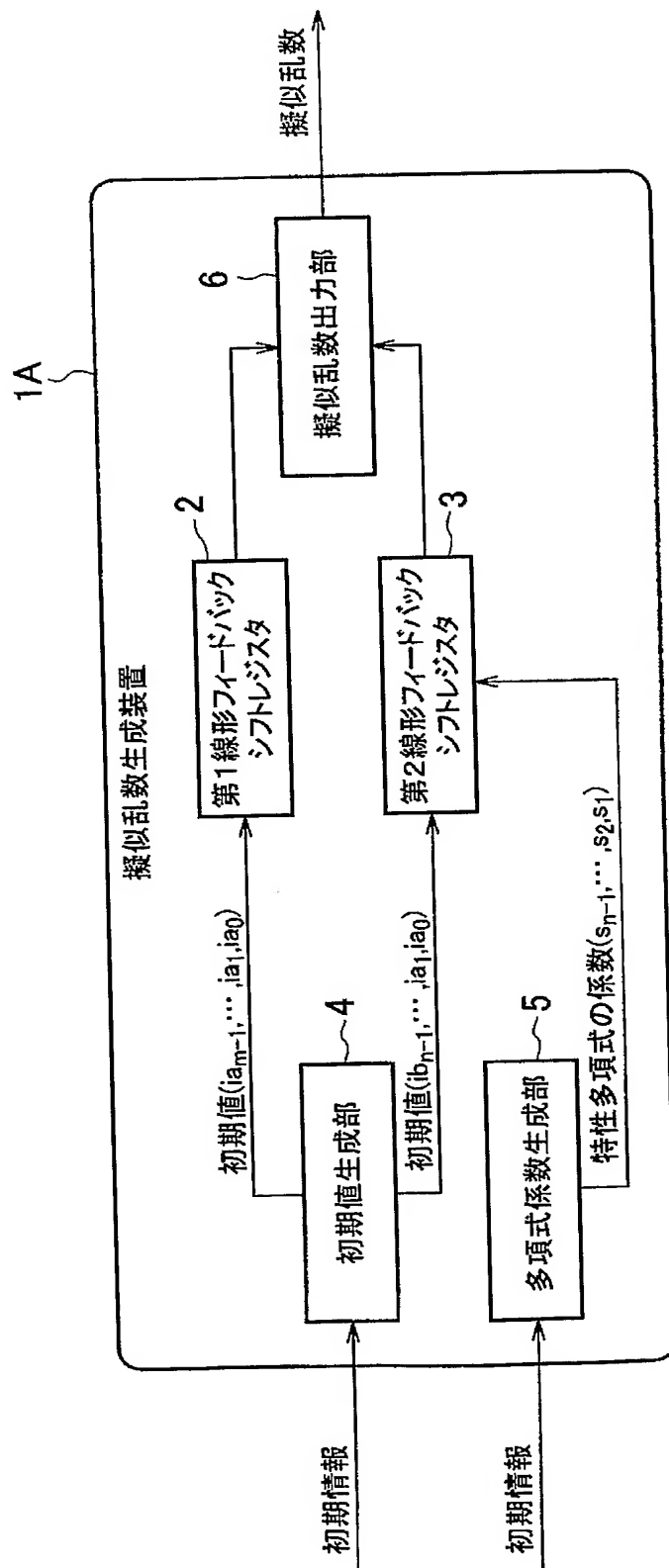
【符号の説明】

【0065】

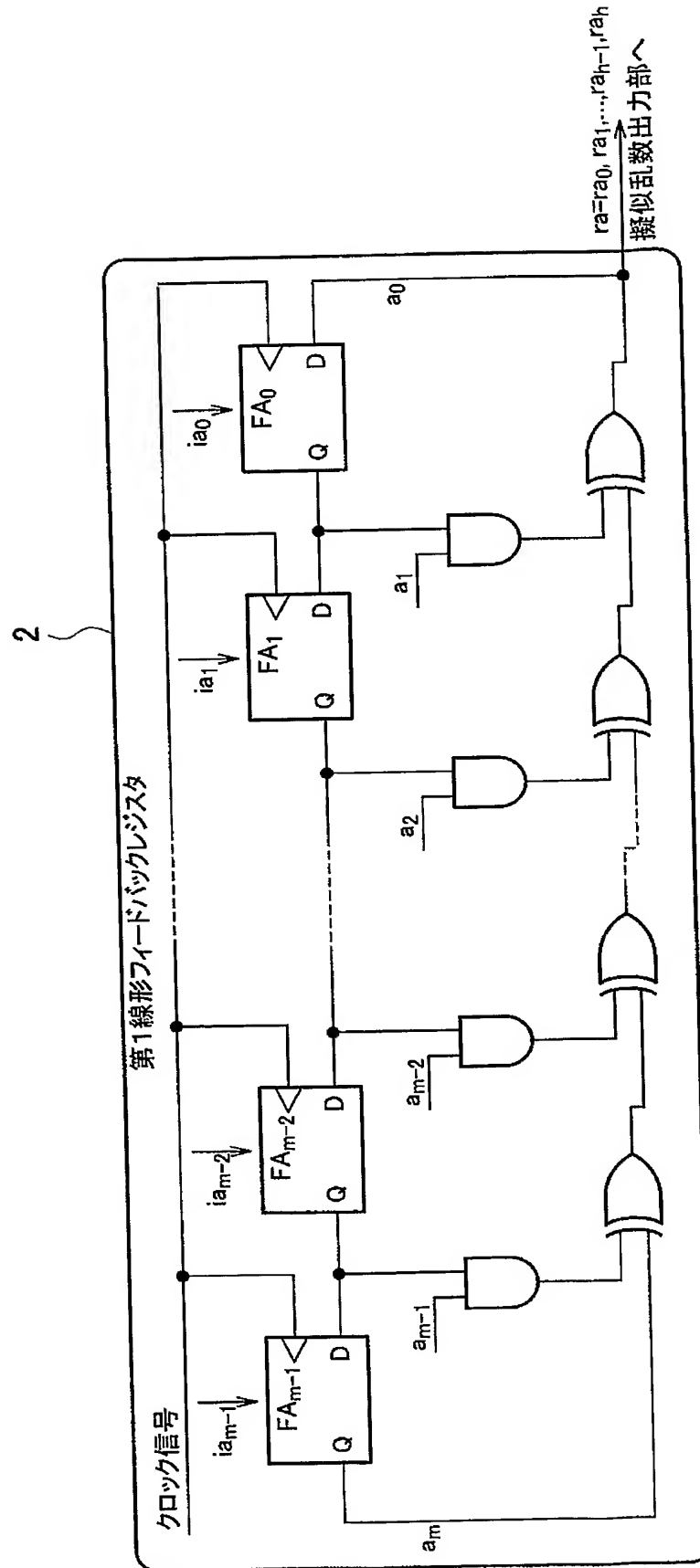
- 1 A、B、C 擬似乱数生成装置
- 2 第 1 線形フィードバックシフトレジスタ
- 3 第 2 線形フィードバックシフトレジスタ
- 4 初期値生成部
- 5 多項式係数生成部

- 6 擬似乱数出力部
- 7 原始多項式選択部
- 8 原始多項式記憶部
- 9 通信部

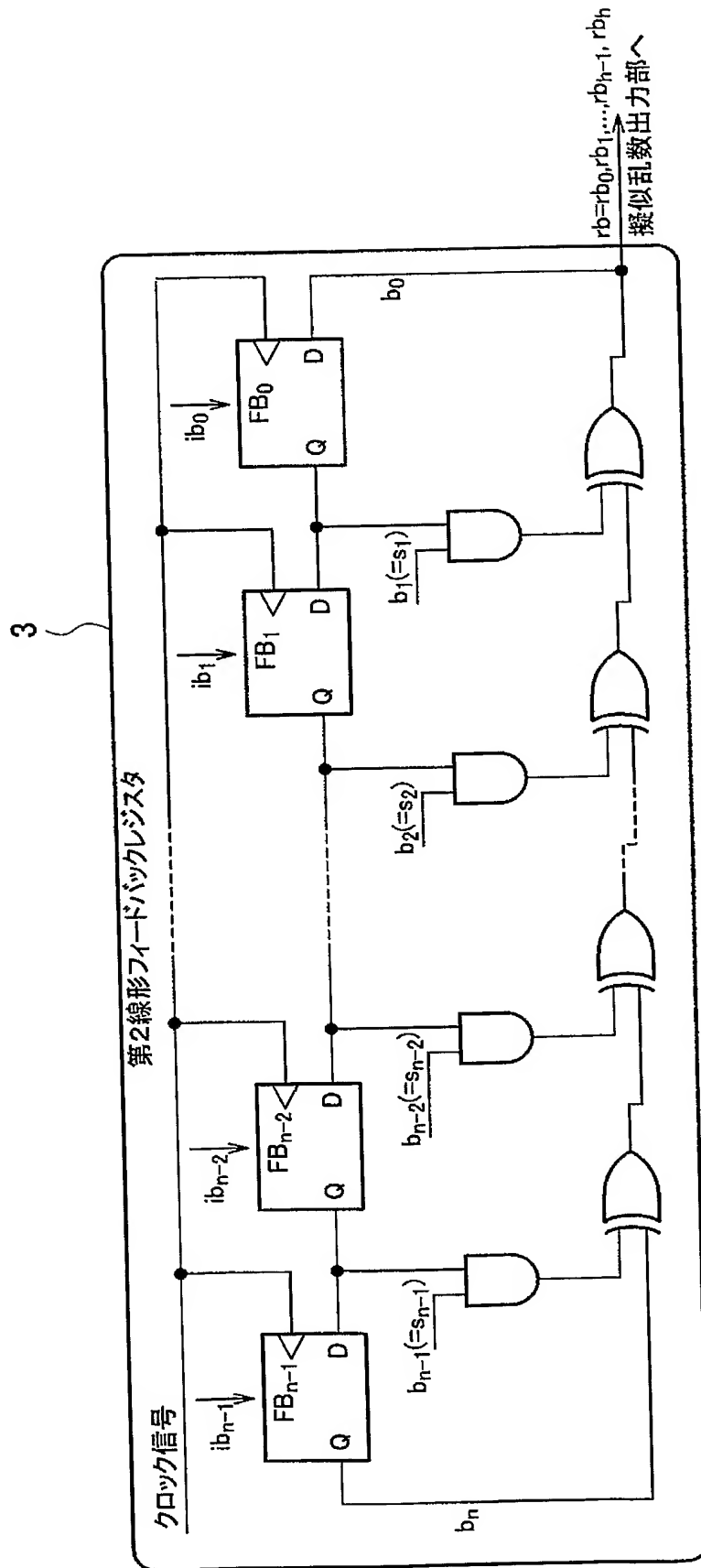
【書類名】 図面
【図 1】



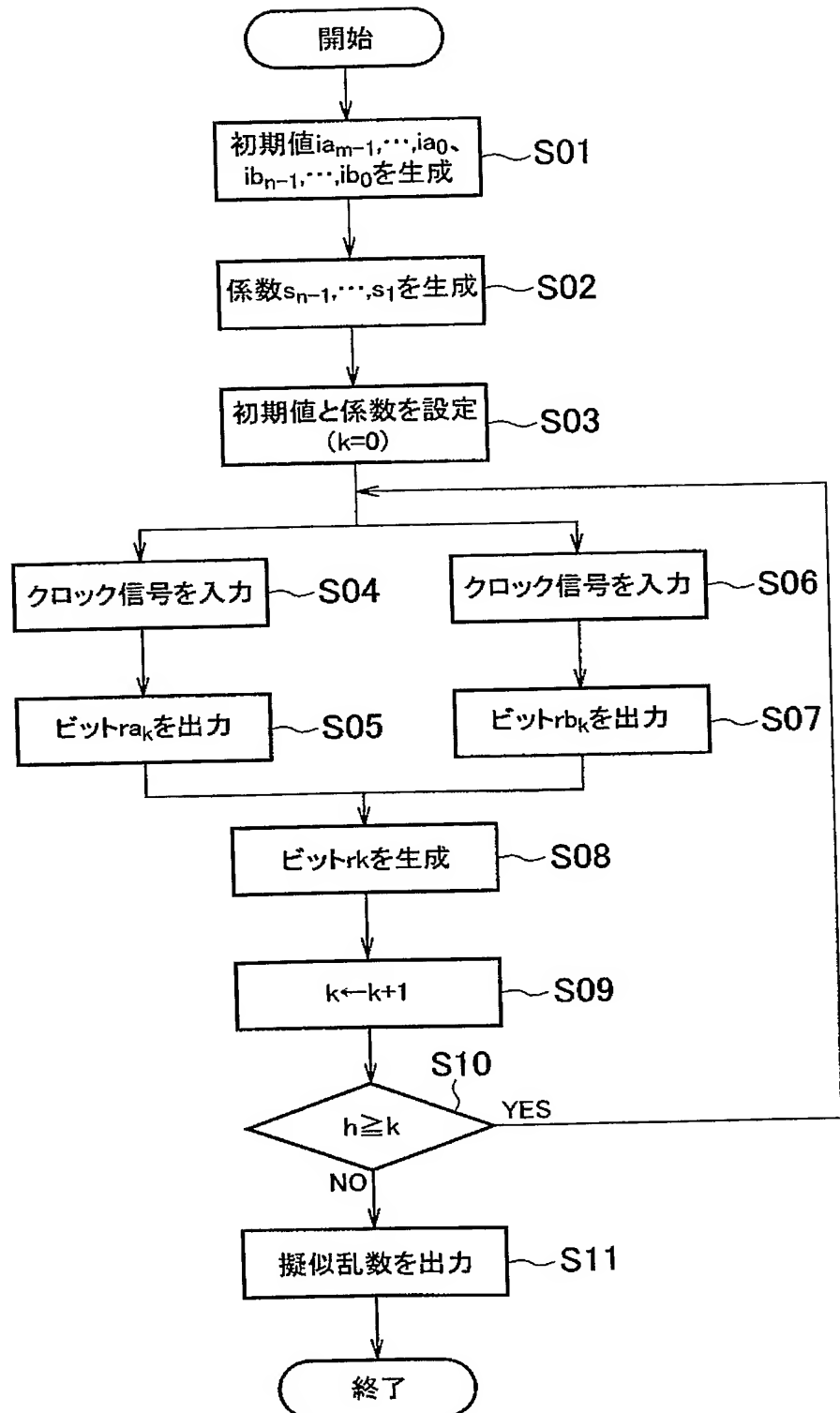
【図 2】



【図 3】



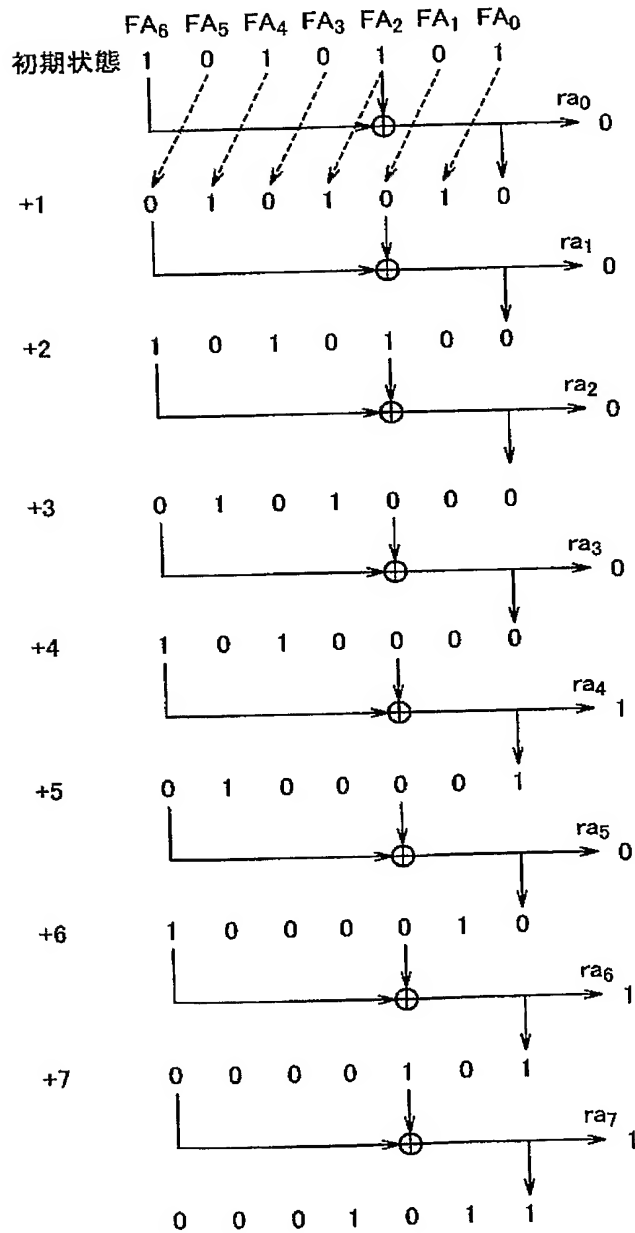
【図 4】



【図 5】

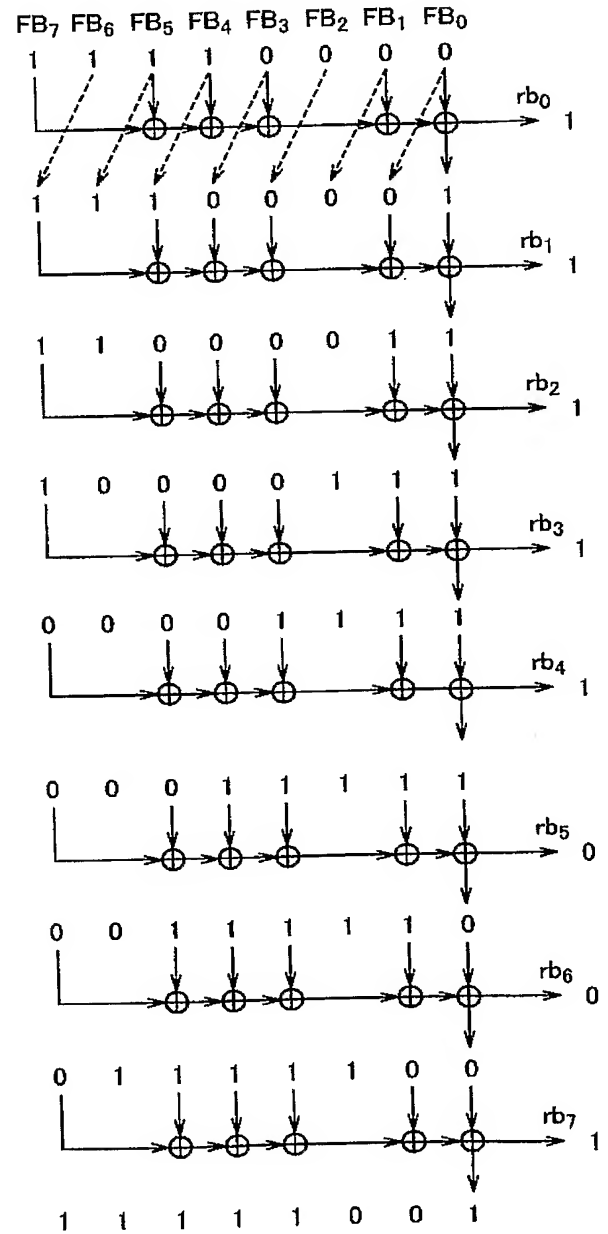
第1線形フィードバックシフトレジスタ

$$x^7+x^3+1 \quad (a_6, a_5, a_4, a_3, a_2, a_1) = (000100)$$

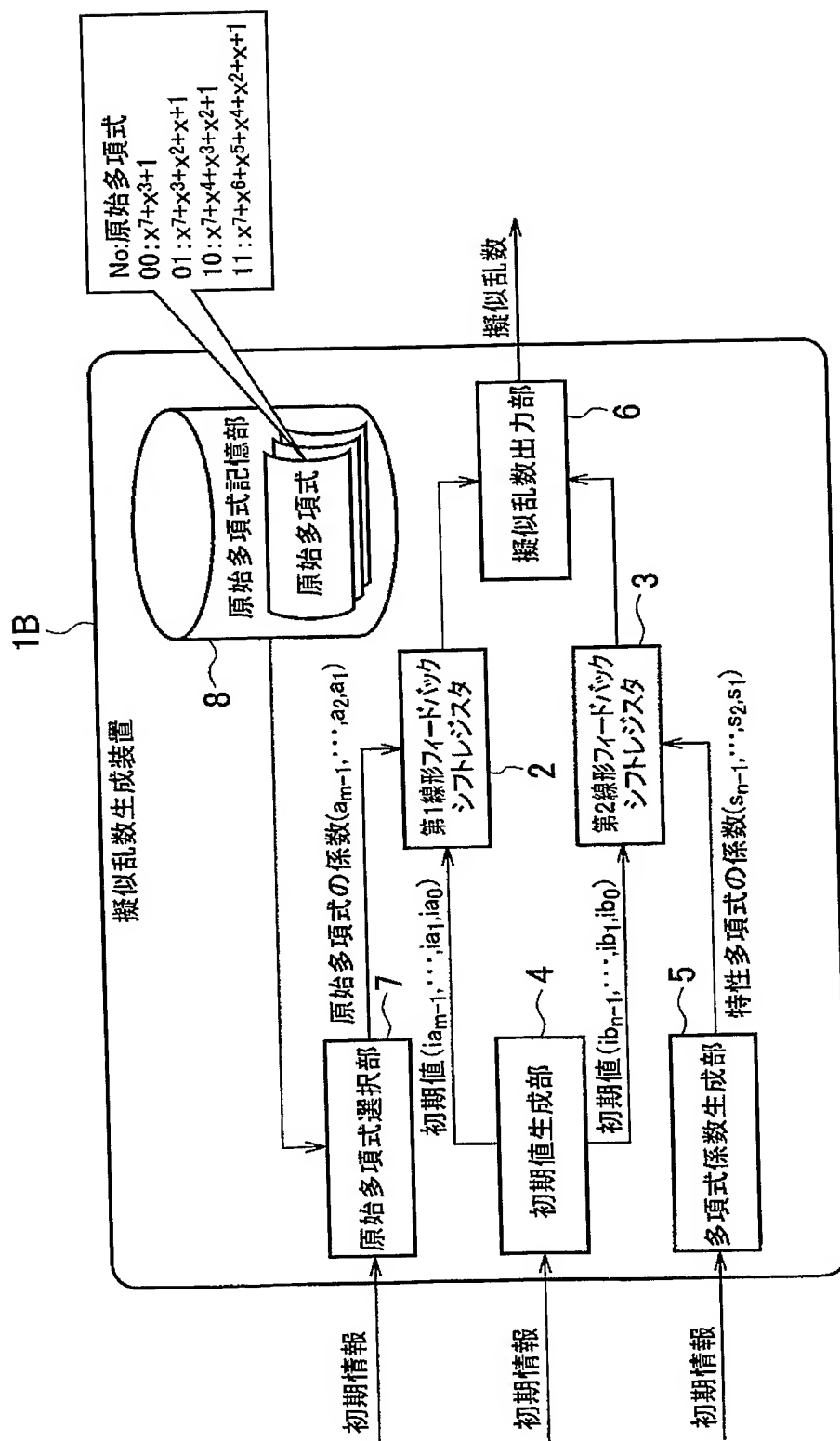


第2線形フィードバックシフトレジスタ

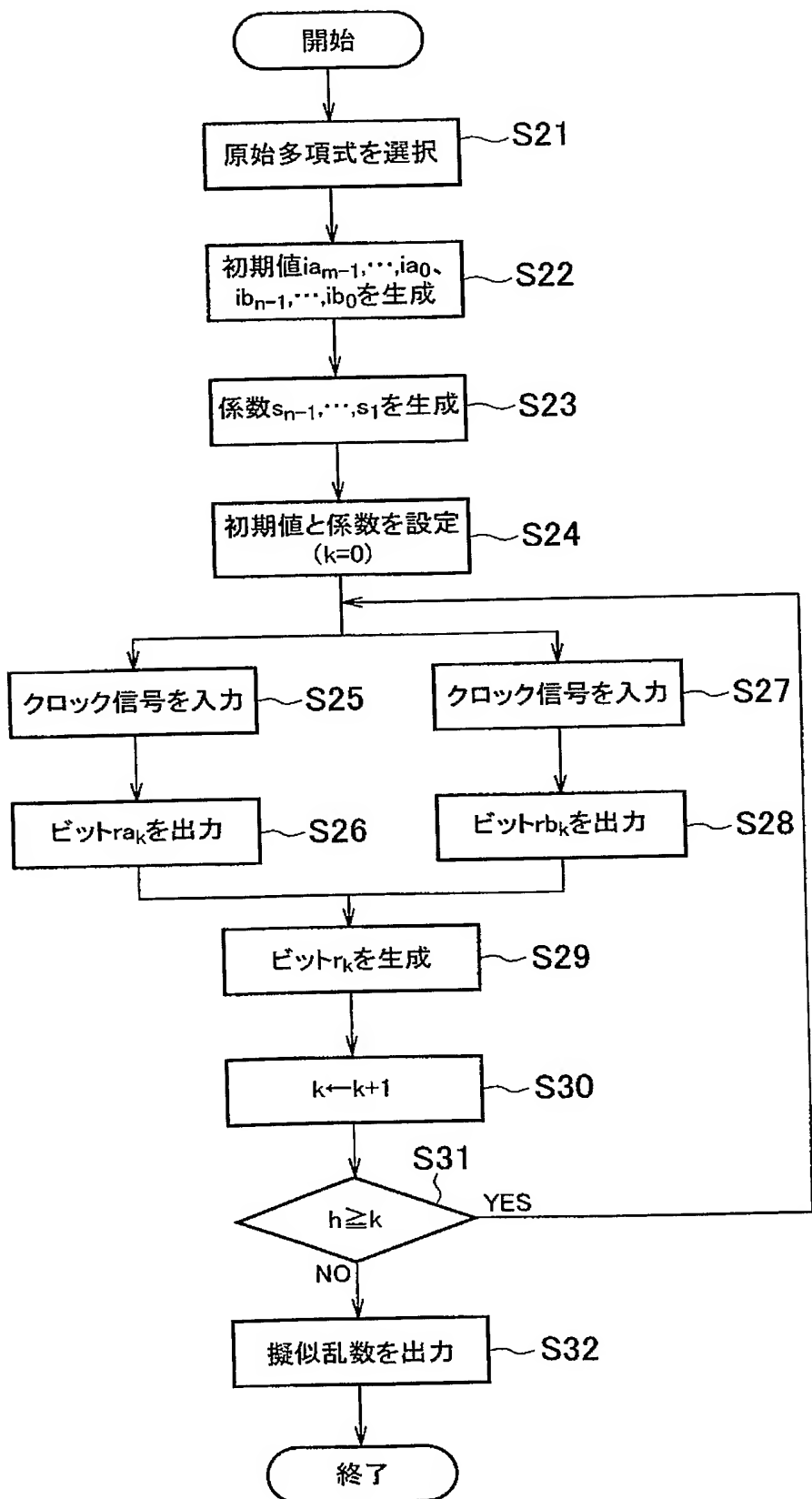
$$x^8+x^6x^5+x^4x^2x+1$$



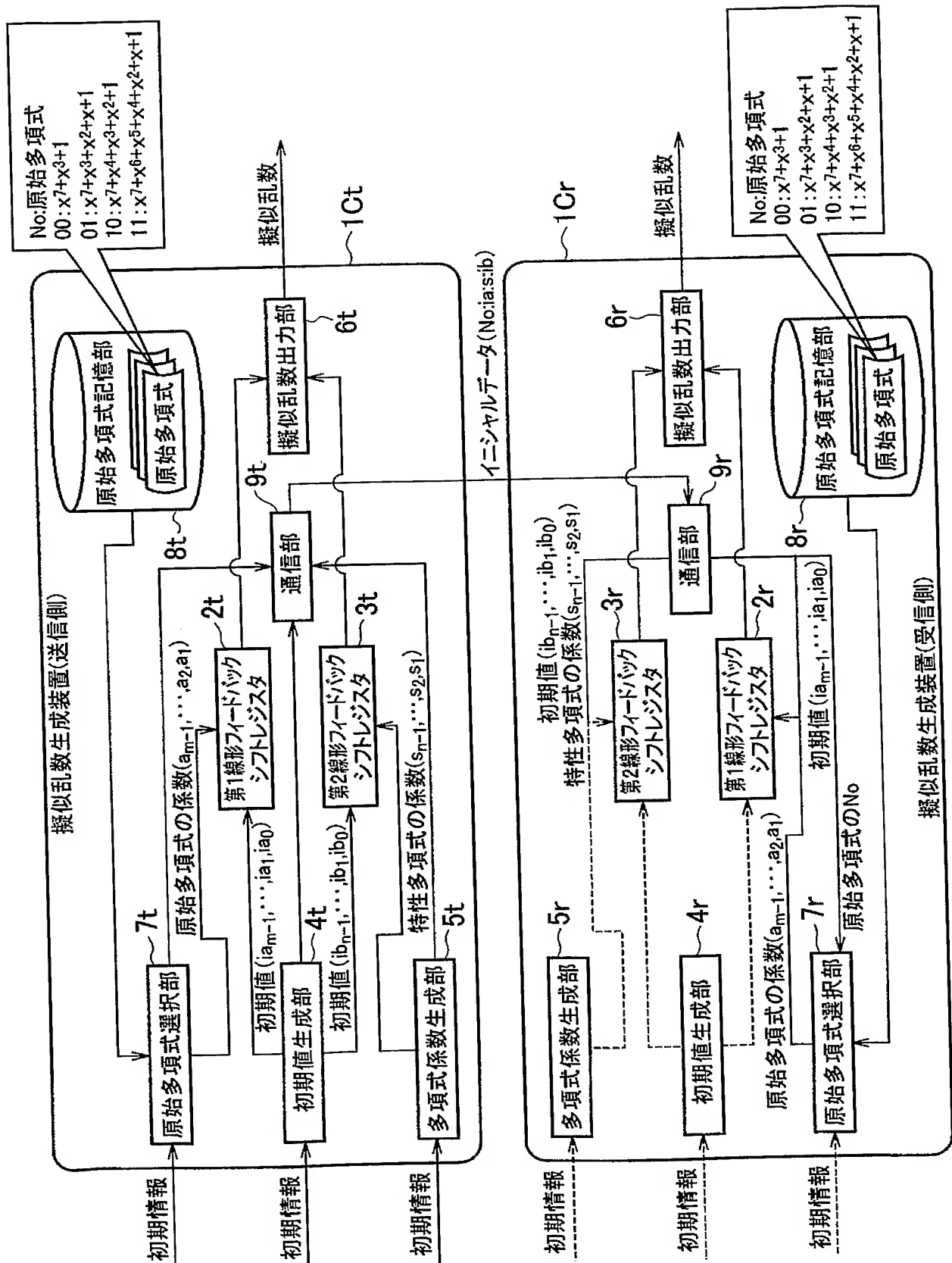
【図 6】



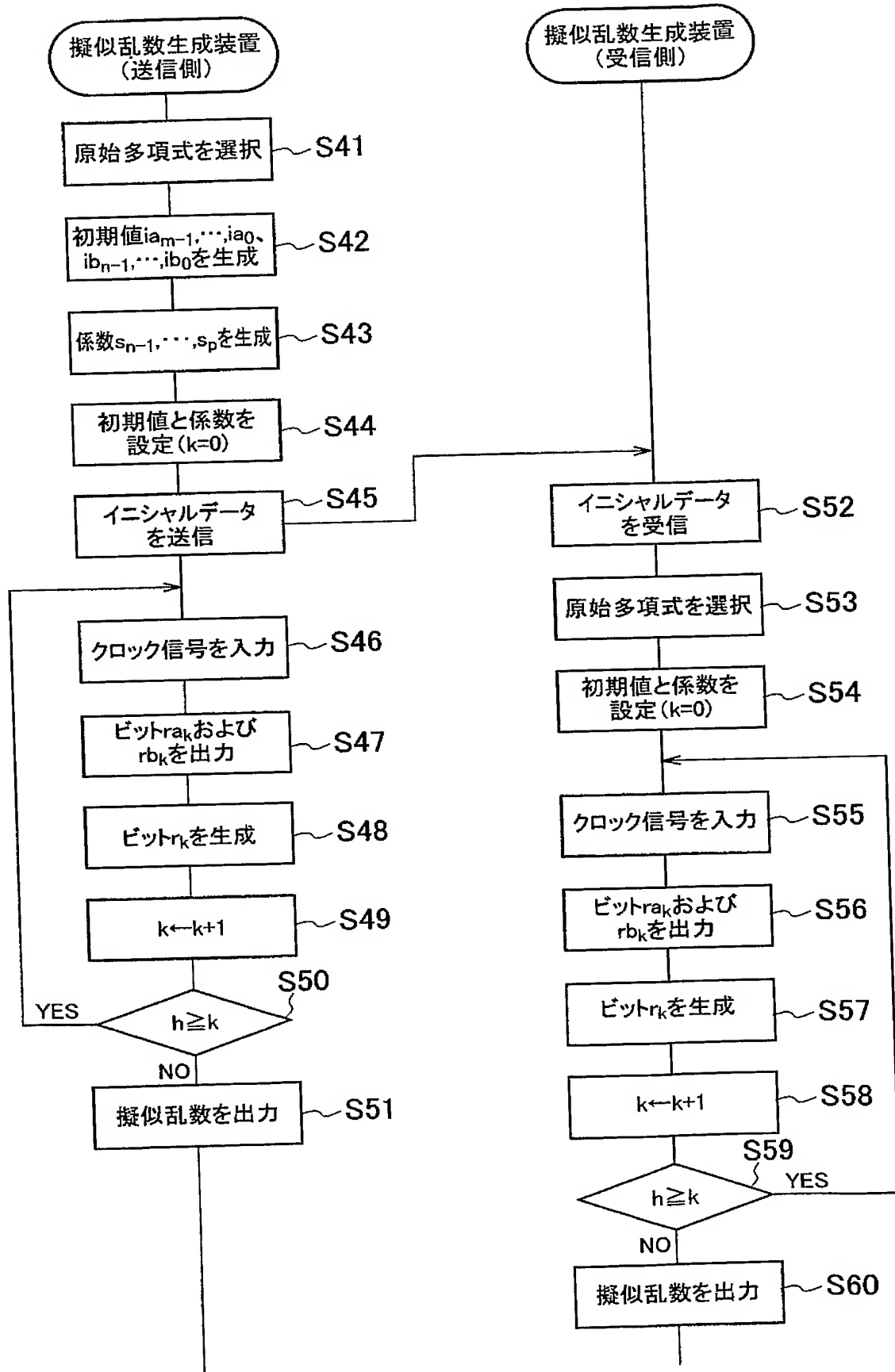
【図 7】



【图 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 擬似乱数列や送受信されるデータを観測されても、その後生成される擬似乱数列の推測が困難な暗号通信に好適な擬似乱数生成装置および擬似乱数生成プログラムを提供する。

【解決手段】 擬似乱数生成装置 1 は、第 1 線形フィードバックシフトレジスタ 2、第 2 線形フィードバックシフトレジスタ 3、初期値生成部 4、多項式係数生成部 5 および擬似乱数出力部 6 を有し、初期値生成部 4 は、初期値を生成し、第 1 線形フィードバックシフトレジスタ 2 および第 2 線形フィードバックシフトレジスタ 3 へ供給し、多項式係数生成部 5 は、特性多項式の係数を生成して第 2 線形フィードバックシフトレジスタ 3 へ供給し、擬似乱数出力部 6 は、第 1 線形フィードバックシフトレジスタ 2 および第 2 線形フィードバックシフトレジスタ 3 から順次出力されるビット列とを基に、各ビットの排他的論理和から擬似乱数列を生成、出力する。

【選択図】 図 1

特願 2 0 0 4 - 0 2 3 3 3 5

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 4 3 2 9]

1. 変更年月日
[変更理由]
住 所
氏 名

1 9 9 0 年 8 月 8 日
新規登録
神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地
日本ビクター株式会社